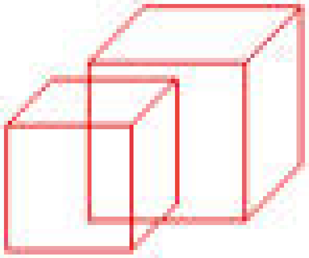
Mathematics and Proof.

Formal proof versus informal proof.

A proof of unprovability needs a formal notion of proof.

The Delic problem (1).



If a cube has height, width and depth 1, then its volume is $1 \times 1 \times 1 = 1^3 = 1$.
If a cube has height, width and depth 2, then its volume is $2 \times 2 \times 2 = 2^3 = 8$.
In order to have volume 2, the height, width and depth of the cube must be $\sqrt[3]{2}$:

$$\sqrt[3]{2} \times \sqrt[3]{2} \times \sqrt[3]{2} = (\sqrt[3]{2})^3 = 2.$$

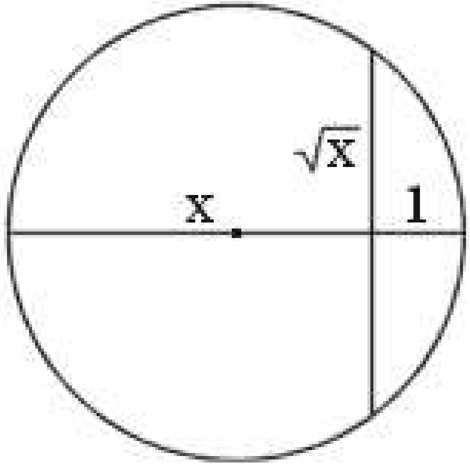
The Delic problem (2).

Question. Given a compass and a ruler that has only integer values on it, can you give a geometric construction of $\sqrt[3]{2}$?

Example. If x is a number that is constructible with ruler and compass, then $\sqrt{x}$ is constructible.

Proof.

If x is the sum of two squares (*i.e.*, $x = n^2 + m^2$), then this is easy by Pythagoras. In general:



The Delic problem (3).

It is easy to see what a positive solution to the Delic problem would be. But a negative solution would require reasoning about all possible geometric constructions.

Geometries (1).

- We call a structure $\langle P, L, I\rangle$ a plane geometry if $I \subseteq P \times L$ is a relation.
- We call the elements of P "points", the elements of L "lines" and we read $pI\ell$ as "p lies on ℓ".
- If ℓ and ℓ^* are lines, we say that ℓ and ℓ^* are parallel if there is no point p such that $pI\ell$ and $pI\ell^*$.
- **Example.** If $P = \mathbb{R}^2$, then we call $\ell \subseteq P$ a line if

$$\ell = \{\langle x, y\rangle \,;\, y = a \cdot x + b\}$$

for some $a, b \in \mathbb{R}$. Let $\mathcal{L}$ be the set of lines. We write $pI\ell$ if $p \in \ell$. Then $\langle P, \mathcal{L}, I\rangle$ is a plane geometry.

Geometries (2).

- (A1) For every $p \neq q \in P$ there is exactly one $\ell \in L$ such that $pI\ell$ and $qI\ell$.
- (A2) For every $\ell \neq \ell^* \in L$, either ℓ and ℓ^* are parallel, or there is exactly one $p \in P$ such that $pI\ell$ and $pI\ell^*$.
- (N) For every $p \in P$ there is an $\ell \in L$ such that p doesn't lie on ℓ and for every $\ell \in L$ there is an $p \in P$ such that p doesn't lie on ℓ.
- (P2) For every $\ell \neq \ell^* \in L$, there is exactly one $p \in P$ such that $pI\ell$ and $pI\ell^*$.

A plane geometry that satisfies (A1), (A2) and (N) is called a plane. A plane geometry that satisfies (A1), (P2) and (N) is called a projective plane.

Geometries (3).

- (A1) For every $p \neq q \in P$ there is exactly one $\ell \in L$ such that $pI\ell$ and $qI\ell$.
- (A2) For every $\ell \neq \ell^* \in L$, either ℓ and ℓ^* are parallel, or there is exactly one $p \in P$ such that $pI\ell$ and $pI\ell^*$.
- (N) For every $p \in P$ there is an $\ell \in L$ such that p doesn't lie on ℓ and for every $\ell \in L$ there is an $p \in P$ such that p doesn't lie on ℓ.

Let $\mathbf{P} := \langle \mathbb{R}^2, \mathcal{L}, \in \rangle$. Then $\mathbf{P}$ is a plane.

- (WE) ("the weak Euclidean postulate") For every $\ell \in L$ and every $p \in P$ such that p doesn't lie on ℓ, there is an $\ell^* \in L$ such that $pI\ell^*$ and ℓ and ℓ^* are parallel.
- (SE) ("the strong Euclidean postulate") For every $\ell \in L$ and every $p \in P$ such that p doesn't lie on ℓ, there is exactly one $\ell^* \in L$ such that $pI\ell^*$ and ℓ and ℓ^* are parallel.

$\mathbf{P}$ is a strongly Euclidean plane.

Geometries (4).

Question. Do (A1), (A2), (N), and (WE) imply (SE)?

It is easy to see what a positive solution would be, but a negative solution would require reasoning over all possible proofs.

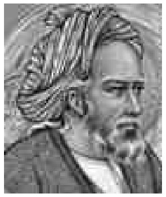
Semantic version of the question. Is every weakly Euclidean plane strongly Euclidean?

Syntactic versus semantic.

	Does Φ imply ψ?	Does every Φ-structure satisfy ψ?
Positive	Give a proof	Check all structures
	$\exists$	$\forall$
Negative	Check all proofs	Give a counterexample
	$\forall$	$\exists$

History of Euclid’s Fifth Postulate (1).

- Ptolemy (c.85-c.165)
- Proclus (411-485)
- Omar Khayyam (1048-1131)



History of Euclid’s Fifth Postulate (1).

- Ptolemy (c.85-c.165)
- Proclus (411-485)
- Omar Khayyam (1048-1131)
- Nasir ad-Din at-Tusi (1201-1274)
- Girard Desargues (1591-1661)

History of Euclid's Fifth Postulate (1).

- Ptolemy (c.85-c.165)
- Proclus (411-485)
- Omar Khayyam (1048-1131)
- Nasir ad-Din at-Tusi (1201-1274)
- Girard Desargues (1591-1661)
- Blaise Pascal (1623-1662)

History of Euclid's Fifth Postulate (1).

- Ptolemy (c.85-c.165)
- Proclus (411-485)
- Omar Khayyam (1048-1131)
- Nasir ad-Din at-Tusi (1201-1274)
- Girard Desargues (1591-1661)
- Blaise Pascal (1623-1662)
- Gerolamo Saccheri (1667-1733): Hypothesis of the acute angle
- Heinrich Lambert (1728-1777)

History of Euclid’s Fifth Postulate (1).

- Ptolemy (c.85-c.165)
- Proclus (411-485)
- Omar Khayyam (1048-1131)
- Nasir ad-Din at-Tusi (1201-1274)
- Girard Desargues (1591-1661)
- Blaise Pascal (1623-1662)
- Gerolamo Saccheri (1667-1733): Hypothesis of the acute angle
- Heinrich Lambert (1728-1777)
- John Playfair (1748-1819)

History of Euclid’s Fifth Postulate (1).

- Ptolemy (c.85-c.165)
- Proclus (411-485)
- Omar Khayyam (1048-1131)
- Nasir ad-Din at-Tusi (1201-1274)
- Girard Desargues (1591-1661)
- Blaise Pascal (1623-1662)
- Gerolamo Saccheri (1667-1733): Hypothesis of the acute angle
- Heinrich Lambert (1728-1777)
- John Playfair (1748-1819)
- Adrien-Marie Legendre (1752-1833): (SE) is equivalent to “the sum of angles of a triangle is equal to $180°$”.

History of Euclid's Fifth Postulate (1).

- Ptolemy (c.85-c.165)
- Proclus (411-485)
- Omar Khayyam (1048-1131)
- Nasir ad-Din at-Tusi (1201-1274)
- Girard Desargues (1591-1661)
- Blaise Pascal (1623-1662)
- Gerolamo Saccheri (1667-1733): Hypothesis of the acute angle
- Heinrich Lambert (1728-1777)
- John Playfair (1748-1819)
- Adrien-Marie Legendre (1752-1833): (SE) is equivalent to "the sum of angles of a triangle is equal to $180°$".

"the scandal of elementary geometry" (D'Alembert 1767)
"In the theory of parallels we are even now not further than Euclid. This is a shameful part of mathematics..." (Gauss 1817)

History of Euclid's Fifth Postulate (2).

Johann Carl Friedrich Gauss (1777-1855)

1817

Nikolai Ivanovich Lobachevsky (1792-1856)

1829

János Bolyai (1802-1860)

1823

Bernhard Riemann (1826-1866).

A non-Euclidean geometry.

Take the usual geometry $\mathbf{P} = \langle \mathbb{R}^2, \mathcal{L}, \in \rangle$ on the Euclidean plane.

Consider $\mathbb{U} := \{x \in \mathbb{R}^2\,;\, \|x\| < 1\}$. We define the restriction of $\mathcal{L}$ to $\mathbb{U}$ by $\mathcal{L}^{\mathbb{U}} := \{\ell \cap \mathbb{U}\,;\, \ell \in \mathcal{L}\}$.

$\mathbf{U} := \langle \mathbb{U}, \mathcal{L}^{\mathbb{U}}, \in \rangle$.

Theorem. $\mathbf{U}$ is a weakly Euclidean plane which is not strongly Euclidean.

Mathematics and real content.

Mathematics getting more abstract...

Imaginary numbers.

Nicolo Tartaglia	Girolamo Cardano
(1499-1557)	(1501-1576)
	

Mathematics and real content.

Mathematics getting more abstract...

Imaginary numbers.

Nicolo Tartaglia	Girolamo Cardano
(1499-1557)	(1501-1576)

Carl Friedrich Gauss (1777-1855)

Ideal elements in number theory.
Richard Dedekind (1831-1916)

Leibniz versus Frege.

Two Slogans.

Leibniz / Boole:	“Natural reasoning is mathematizable.”
Frege	“Mathematics is logic.”

Syllogistics versus Propositional Logic.

Deficiencies of Syllogistics:

Not expressible:

Every X is a Y and a Z. *Ergo...* Every X is a Y.

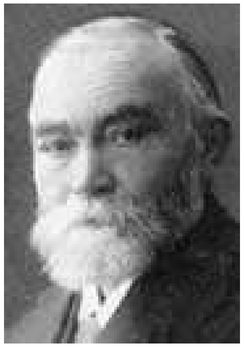
Deficiencies of Propositional Logic:

- $X\mathrm{a}Y$ can be represented as $Y \rightarrow X$.
- $X\mathrm{e}Y$ can be represented as $Y \rightarrow \neg X$.

Not expressible:

$X\mathrm{i}Y$ and $X\mathrm{o}Y$.

Frege.

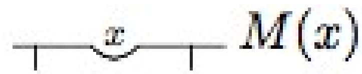
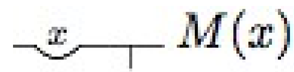
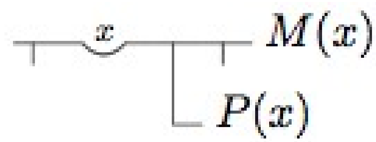


Gottlob Frege
1848 - 1925

- Studied in Jena and Göttingen.
- Professor in Jena.
- *Begriffsschrift* (1879).
- *Grundgesetze der Arithmetik* (1893/1903).

“Every good mathematician is at least half a philosopher, and every good philosopher is at least half a mathematician. (G. Frege)”

Frege's logical framework.

"Everything is M"		$\forall x\, M(x)$
"Something is M"		$\exists x\, M(x) \equiv \neg\forall x\, \neg M(x)$
"Nothing is M"		$\forall x\, \neg M(x)$
"Some P is an M"		$\exists x\, (P(x) \wedge M(x))$ $\equiv \neg\forall x\, (P(x) \rightarrow \neg M(x))$

Second order logic allowing for quantification over properties.

Frege's importance.

- Notion of a formal system.
- Formal notion of proof in a formal system.
- Analysis of number-theoretic properties in terms of second-order properties.
  $\rightsquigarrow$ Russell's Paradox
  (*Grundlagekrise der Mathematik*)

Hilbert (1).

David Hilbert (1862-1943)
Student of Lindemann
1886-1895 Königsberg
1895-1930 Göttingen

1899: *Grundlagen der Geometrie*

“*Man muss jederzeit an Stelle von ‘Punkten’, ‘Geraden’, ‘Ebenen’ ‘Tische’, ‘Stühle’, ‘Bierseidel’ sagen können.*”
“It has to be possible to say ‘tables’, ‘chairs’ and ‘beer mugs’ instead of ‘points’, ‘lines’ and ‘planes’ at any time.”

Hilbert (2).

GRUNDZÜGE
DER THEORETISCHEN
LOGIK

VON

D. HILBERT

UND

W. ACKERMANN

BERLIN
VERLAG VON JULIUS SPRINGER
1928

1928: **Hilbert-Ackermann**
Grundzüge der Theoretischen Logik

Wilhelm Ackermann (1896-1962)

First order logic (1).

A first-order language $\mathcal{L}$ is a set $\{\dot{\mathrm{f}}_i\,;\, i \in I\} \cup \{\dot{\mathrm{R}}_j\,;\, j \in J\}$ of function symbols and relation symbols together with a signature $\sigma : I \cup J \to \mathbb{N}$.

- $\sigma(\dot{\mathrm{f}}_i) = n$ is interpreted as "$\dot{\mathrm{f}}_i$ represents an n-ary function".
- $\sigma(\dot{\mathrm{R}}_i) = n$ is interpreted as "$\dot{\mathrm{R}}_i$ represents an n-ary relation".

In addition to the symbols from $\mathcal{L}$, we shall be using the logical symbols $\forall$, $\exists$, $\wedge$, $\vee$, $\to$, $\neg$, $\leftrightarrow$, equality $=$, and a set of variables Var.

First order logic (2).

We fi x a fi rst-order language $\mathcal{L} = \{\dot{\mathrm{f}}_i \,;\, i \in I\} \cup \{\dot{\mathrm{R}}_j \,;\, j \in J\}$ and a signature $\sigma : I \cup J \to \mathbb{N}$.

Definition of an $\mathcal{L}$-term.

- Every variable is an $\mathcal{L}$-term.
- If $\sigma(\dot{\mathrm{f}}_i) = n$, and $t_1, ..., t_n$ are $\mathcal{L}$-terms, then $\dot{\mathrm{f}}_i(t_1, ..., t_n)$ is an $\mathcal{L}$-term.
- Nothing else is an $\mathcal{L}$-term.

Example. Let $\mathcal{L} = \{\dot{\times}\}$ be a first order language with a binary function symbol.

- $\dot{\times}(x, x)$ is an $\mathcal{L}$-term (normally written as $x \dot{\times} x$, or x^2).
- $\dot{\times}(\dot{\times}(x, x), x)$ is an $\mathcal{L}$-term (normally written as $(x \dot{\times} x) \dot{\times} x$, or x^3).

First order logic (3).

Definition of an $\mathcal{L}$-formula.

- If t and t^* are $\mathcal{L}$-terms, then $t = t^*$ is an $\mathcal{L}$-formula.
- If $\sigma(\dot{\mathrm{R}}_i) = n$, and $t_1, ..., t_n$ are $\mathcal{L}$-terms, then $\dot{\mathrm{R}}_i(t_1, ..., t_n)$ is an $\mathcal{L}$-formula.
- If φ and ψ are $\mathcal{L}$-formulae and x is a variable, then $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \to \psi$, $\varphi \leftrightarrow \psi$, $\forall x\,(\varphi)$ and $\exists x\,(\varphi)$ are $\mathcal{L}$-formulae.
- Nothing else is an $\mathcal{L}$-formula.

An $\mathcal{L}$-formula without free variables is called an $\mathcal{L}$-sentence.

Semantics (1).

We fix a first-order language $\mathcal{L} = \{\dot{\mathrm{f}}_i \,;\, i \in I\} \cup \{\dot{\mathrm{R}}_j \,;\, j \in J\}$ and a signature $\sigma : I \cup J \to \mathbb{N}$.

A tuple $\mathbf{X} = \langle X, \langle f_i \,;\, i \in I\rangle, \langle R_j \,;\, j \in J\rangle\rangle$ is called an $\mathcal{L}$-structure if f_i is an $\sigma(\dot{\mathrm{f}}_i)$-ary function on X and R_i is an $\sigma(\dot{\mathrm{R}}_i)$-ary relation on X.

An X-interpretation is a function $\iota : \mathrm{Var} \to X$.

If ι is an X-interpretation and $\mathbf{X}$ is an $\mathcal{L}$ then ι extends to a function $\hat{\iota}$ on the set of all $\mathcal{L}$-terms.

If $\mathbf{X}$ is an $\mathcal{L}$-structure and ι is an X-interpretation, we define a semantics for all $\mathcal{L}$-formulae by recursion.

Semantics (2).

If $\mathbf{X}$ is an $\mathcal{L}$-structure and ι is an X-interpretation, we defi ne a semantics for all $\mathcal{L}$-formulae by recursion.

- $\mathbf{X}, \iota \models t = t^*$ if and only if $\hat{\iota}(t) = \hat{\iota}(t^*)$.
- $\mathbf{X}, \iota \models \dot{\mathrm{R}}_j(t_1, ..., t_n)$ if and only if $R(\hat{\iota}(t_1), ..., \hat{\iota}(t_n))$.
- $\mathbf{X}, \iota \models \varphi \wedge \psi$ if and only if $\mathbf{X}, \iota \models \varphi$ and $\mathbf{X}, \iota \models \psi$.
- $\mathbf{X}, \iota \models \neg\varphi$ if and only if it is not the case that $\mathbf{X}, \iota \models \varphi$.
- $\mathbf{X}, \iota \models \forall x\,(\varphi)$ if and only if for all X-interpretations ι^* with $\iota \sim_x \iota^*$, we have $\mathbf{X}, \iota^* \models \varphi$.
- $\mathbf{X} \models \varphi$ if and only if for all X-interpretations ι, we have $\mathbf{X}, \iota \models \varphi$.

Object Language $\leftrightarrow$ Metalanguage.

Semantics (3).

Object Language $\leftrightarrow$ Metalanguage.

Let $\mathbf{X}$ be an $\mathcal{L}$-structure. The theory of $\mathbf{X}$, $\mathrm{Th}(\mathbf{X})$, is the set of all $\mathcal{L}$-sentences φ such that $\mathbf{X} \models \varphi$.

Under the assumption that the *tertium non datur* holds for the metalanguage, the theory of $\mathbf{X}$ is always complete:

For every sentence φ, we either have $\varphi \in \mathrm{Th}(\mathbf{X})$ or $\neg\varphi \in \mathrm{Th}(\mathbf{X})$.

Deduction (1).

Let Φ be a set of $\mathcal{L}$-sentences. A Φ-proof is a finite sequence $\langle \varphi_1, ..., \varphi_n \rangle$ of $\mathcal{L}$-formulae such that for all i, one of the following holds:

- $\varphi_i \equiv t = t$ for some $\mathcal{L}$-term t,
- $\varphi_i \in \Phi$, or
- there are $j, k < i$ such that φ_j and φ_k are the premisses and φ_i is the conclusion in one of the rows of the following table.

Premisses		Conclusion
$\varphi \wedge \psi$		φ
$\varphi \wedge \psi$		ψ
φ	ψ	$\varphi \wedge \psi$
φ	$\neg\varphi$	ψ
$\varphi \to \psi$	$\neg\varphi \to \psi$	ψ
$\forall x\,(\varphi)$		$\varphi\frac{s}{x}$
$\varphi\frac{y}{x}$		$\forall x\,(\varphi))$
$t = t^*$	$\varphi\frac{t}{x}$	$\varphi\frac{t^*}{x}$

Deduction (2).

If Φ is a set of $\mathcal{L}$-sentences and φ is an $\mathcal{L}$-formula, we write $\Phi \vdash \varphi$ if there is a Φ-proof in which φ occurs.

We call a set Φ of sentences a theory if whenever $\Phi \vdash \varphi$, then $\varphi \in \Phi$ ("Φ is deductively closed").

Example. Let $\mathcal{L} = \{\leq\}$ be the language of partial orders. Let $\Phi_{\mathrm{p.o.}}$ be the axioms of partial orders, and let Φ be the deductive closure of $\Phi_{\mathrm{p.o.}}$. Φ is not a complete theory, as the sentence $\forall x \forall y (x \leq y \vee y \leq x)$ is not an element of Φ, but neither is its negation.

Completeness.

Kurt Gödel (1906-1978)

Semantic entailment. We write $\Phi \models \varphi$ for "whenever $\mathbf{X} \models \Phi$, then $\mathbf{X} \models \varphi$".

Gödel Completeness Theorem (1929).

$\Phi \vdash \varphi$ if and only if $\Phi \models \varphi$.

"there is a Φ-proof of φ" "for all $\mathbf{X} \models \Phi$, we have $\mathbf{X} \models \varphi$"

$\Phi \nvdash \varphi$ if and only if $\Phi \not\models \varphi$.

"no Φ-proof contains φ" "there is some $\mathbf{X} \models \Phi \wedge \neg\varphi$"

Applications (1).

The Model Existence Theorem.

If Φ is consistent (*i.e.*, $\Phi \nvdash \bot$), then there is a model $\mathbf{X} \models \Phi$.

The Compactness Theorem.

Let Φ be a set of sentences. If every finite subset of Φ has a model, then Φ has a model.

Proof. If Φ doesn't have a model, then it is inconsistent by the **Model Existence Theorem**. So, $\Phi \vdash \bot$, *i.e.*, there is a Φ-proof P of $\bot$.
But P is a finite object, so it contains only finitely many elements of Φ. Let Φ_0 be the set of elements occurring in P. Clearly, P is a Φ_0-proof of $\bot$, so Φ_0 is inconsistent. Therefore Φ_0 cannot have a model. q.e.d.

Applications (2).

The Compactness Theorem. Let Φ be a set of sentences. If every finite subset of Φ has a model, then Φ has a model.

Corollary 1. Let Φ be a set of sentences that has arbitrary large finite models. Then Φ has an infinite model.

Proof. Let $\psi_{\geq n}$ be the formula stating "there are at least n different objects". Let $\Psi := \{\psi_{\geq n}\,;\, n \in \mathbb{N}\}$. The premiss of the theorem says that every finite subset of $\Phi \cup \Psi$ has a model. By compactness, $\Phi \cup \Psi$ has a model. But this must be infinite. q.e.d.

Let $\mathcal{L} := \{\leq\}$ be the first order language with one binary relation symbol. Let $\Phi_{\text{p.o.}}$ be the axioms of partial orders.

Corollary 2. There is no sentence σ such that for all partial orders $\mathbf{P}$, we have

$$\mathbf{P} \text{ is finite if and only if } \mathbf{P} \models \sigma.$$

[If σ is like this, then **Corollary 1** can be applied to $\Phi_{\text{p.o.}} \cup \{\sigma\}$.]